EXHIBIT 1

INTL · FCStone®

Commodities · Global Payments · Foreign Exchange · Securities

Acceptable Use Policy

INTL FCSTONE Inc.
708 Third Avenue
Suite 1500
New York, NY 10017
+1 (212) 485-3500

Version: 1.0
Date: October 2017

Document Control

Title	Acceptable Use Policy
Owner	Information Security Risk, Governance
Author	David Hall - Head of Information Security Risk, Governance
Contributors	HR, Legal
Protective Marking	Commercial in Confidence
Reviewer / Approver	Jim Richey - Global Head of Human Resources
Review Period	12 Months (Annually)
Target Audience	All Staff, Regulators, Contractors and Vendors

If you have any questions relating to this document, please contact –

David Hall – Global Head of Information Security & IT Governance
120, London Wall, London, EC2Y 5ET
Tel +44 (0) 203 580 6372
Email: david.hall@intlfcstone.com

This document has been developed to meet business, statutory and or regulatory requirements; and is binding on all companies trading as INTL FCSTONE.

It is the responsibility of Senior Management to ensure that any policies and procedures relating to this document or area of responsibility are effectively communicated, implemented and monitored.

*This document forms part of INTL FCSTONE's **Information Security Policy** and as such cannot be changed in any way without formal authorization.*

*To propose a change to this document, a change request is required to be submitted to the document owner for review and approval. For more information please refer to the **Document and Records Management Policy**.*

Contents

1.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and systems at INTL FCStone (The Company). Effective security is a team effort involving the participation and support of every The Company employee who deals with information and/or information systems. It is the responsibility of every computer user to know these rules, and to conduct their activities accordingly. These rules are in place to protect both the employee and the company.

IT resources and systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and FTP, are the property of The Company. These systems are to be used for business purposes in serving the interests of The Company, and of its clients in the course of normal operations.

Inappropriate use may expose The Company to risks including virus attacks, compromise of network systems and services, and legal repercussions, therefore any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2.0 Scope

This policy applies to the use of information, electronic and computing devices, and network resources used to conduct The Company's business or interact with network and business systems, whether owned or leased by The Company, the employee, or a third party.

All employees, contractors, consultants, temporary employees, and any other users of The Company's systems (Users) are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with The Company policies and standards, and local laws and regulation.

This policy applies to all Users at The Company including all personnel affiliated with third parties. This policy governs all IT resources and communications systems owned by or available to The Company, and all use of such resources and systems when accessed using an employee's own resources, including but not limited to:

- E-mail systems and accounts;
- Internet and intranet access;
- Telephones and voicemail systems, including wired and mobile phones/smartphones;
- Printers, photocopiers and scanners;
- Fax machines, e-fax systems;
- All other associated computer, network and communications systems, hardware, peripherals and software, including network key fobs and other devices;
- Closed-circuit television (CCTV) and all other physical security systems and devices, including access key cards and fobs.

3.0 Policy

3.1 No Expectation of Privacy.

All contents of The Companys IT resources and communications systems are the property of The Company. Therefore, employees should have no expectation of privacy whatsoever in any message, files, data, document, facsimile, telephone conversation, social media post, conversation or message, or any other kind or form of information or communication

transmitted to, received or printed from, or stored or recorded on The Companys electronic information and communications systems.

You are expressly advised that in order to prevent against misuse, The Company reserves the right to monitor, intercept and review, without further notice, all employee's activities using the company's IT resources and communications systems, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voice mail recordings, instant messages and internet and social media postings and activities, and you consent to such monitoring by your acknowledgement of this policy and your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The Company may also store copies of such data and communications for a period of time after they are created, and may delete such copies from time to time without notice.

Do not use The Company's IT resources and communications systems for any matter that you desire to be kept private or confidential from the company.

3.2 Security, Access and Passwords

Security of The Company's IT resources and communications systems is the responsibility of the Information Technology (IT) Department, including approval and control of Users access to systems and suspension or termination of access in cases of misuse and when a User is no longer an employee or otherwise ineligible to use the systems.

It is the responsibility of each employee to adhere to IT security guidelines including but not limited to the creation, format and scheduled changes of passwords. All user names, pass codes, passwords, and information used or stored on The Company's computers, networks and systems are the property of The Company. No employee may use a user name, pass code, password or method of encryption that has not been issued to that employee or authorized in advance by The Company.

No employee shall share user names, pass codes or passwords with any other person. Employee's shall immediately inform the IT Helpdesk if he/she knows or suspects that any user name, pass code or password has been improperly shared or used, or that IT security has been violated in any way.

3.3 General Use and Ownership

a) The Company proprietary information stored on electronic and computing devices whether owned or leased by the Company, the employee or a third party, remains the sole property of The Company;
b) Users must ensure that proprietary information is protected in accordance with Data Protection standards;
c) Users have a responsibility to promptly report the theft, loss or unauthorised disclosure of The Company proprietary information;
d) Users may access, use or share The Companys proprietary information only to the extent it is authorised and necessary to fulfil their assigned duties;

e) Users are responsible for exercising good judgment regarding reasonable personal use of the Internet, if there is any uncertainty, employees should consult their Line Manager;
f) For security and network maintenance purposes, authorised employees or third party representatives of The Company may monitor equipment, systems and network traffic at any time;
g) The Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.4 Security and Proprietary Information

a) All mobile and computing devices that connect to the internal network must comply with the Access Control Policy;
b) System level and user level passwords must comply with the Password Management Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited;
c) All devices must be secured with a password-protected screensaver with the automatic activation feature set to 5 minutes or less. You must lock the screen or log off when the device is unattended;
d) Postings by employees from The Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of The Company, unless posting is in the course of business duties;
e) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

For more information please refer to; ***Social Media Policy***
Access Control Policy
Password Management Policy

3.5 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of The Company authorised to engage in any activity that is illegal under local or international law while utilising The Companys IT resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

3.5.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by The Company;

b) Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which The Company or the end user does not have an active license is strictly prohibited;
c) Accessing data, a server or an account for any purpose other than conducting The Company business is prohibited;
d) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Appropriate management should be consulted prior to export of any material that is in question;
e) Purposely introducing malicious programs into the network or a server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);
f) Revealing account passwords to others or allowing use of your account by others. This includes family and other household members when work is being undertaken at home;
g) Using a Company computing asset to actively engage in procuring or transmitting material that portrays pornography, racism, sexuality or religious hatred, or is in violation of hostile workplace laws in the user's local jurisdiction;
h) Conducting or soliciting illegal activities, or making fraudulent offers of products, items, or services originating from any Company account;
i) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the ‘user’ is not an intended recipient or logging into a server or account that the ‘user’ is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
j) Port scanning or security scanning is expressly prohibited unless prior notification to IT Security is made;
k) Executing any form of network monitoring which will intercept data not intended for the User, unless this activity is a part of the User’s normal job/duty;
l) Circumventing user authentication or security of any host, network or account;
m) Introducing honeypots, honey-nets, or similar technology on The Companys network;
n) Interfering with or denying service to any user other than the Users’ host (for example, denial of service attack);
o) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
p) Providing information about, or lists of, employees to parties outside The Company.

3.5.2 Email and Communication Activities

When using company resources to access and use the Internet, Users must not:

a) Send unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);
b) Conduct any form of harassment via email, telephone or text, whether through language, frequency, or size of messages;
c) Use any other Company email address, other than that of the Users account, with the intent to harass or to collect replies;
d) Create or forward "chain letters", "Ponzi" or other "pyramid" schemes of any type;
e) Post the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
f) Access

3.5.3 Blogging and Social Media

a) Users engaged in blogging or social media activities using The Company's property and systems, are subject to the terms and restrictions set forth in this Policy. The use of The Company's systems to engage in blogging or social media activities is acceptable, provided that it is done pursuant to The Company's marketing initiatives, undertaken in a professional and responsible manner, does not violate The Company's policy and is not detrimental to the Company's best interests. Blogging or social media activities from The Company's systems may be subject to monitoring;
b) Users are prohibited from revealing any confidential or proprietary information, trade secrets or any other material when engaged in blogging or social media activities;
c) Users shall not engage in any blogging or social media activities that may harm or tarnish the image, reputation and/or goodwill of The Company and/or any of its employees. Users are prohibited from making any discriminatory, disparaging, defamatory or harassing comments when engaged in blogging or social media activities or otherwise engaging in any conduct prohibited by The Company's Non-Discrimination and Anti-Harassment Policies.
d) Users may not attribute personal statements, opinions or beliefs to The Company when engaged in blogging or social media activities. If a User is expressing his or her beliefs and/or opinions, the User may not, expressly or implicitly, represent themselves as an employee or representative of The Company. Users assume any and all risk associated with blogging or social media activities.
e) Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, The Company's logos and any other intellectual property may not be used in connection with any blogging or social media activity, unless approved as part of their daily duties.

For more information please refer to : ***Social Media Policy***

4.0 Monitoring

In order to ensure compliance with this policy, The Company reserves the right to use monitoring software to monitor, record and examine the content of emails; as well as monitor and/or restrict internet in compliance with the Company's policies and any applicable laws and regulations. Such monitoring will be undertaken only by authorised employees.

5.0 Sanctions

Employees that receive any e-mails to their work e-mail address corresponding to any of the unacceptable or inappropriate behaviours listed above, should, in the first instance, contact their Line Manager or Department Head. Any breach of the policy provisions outlined above may be subject to Company's disciplinary procedures.